UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

RALPH PENA, individually and on behalf of all others similarly situated, Plaintiff, v. BRITISH AIRWAYS, PLC (UK), Defendant.	**Civil Action No.** 18-cv-6278 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Ralph Pena (ñPlaintiffò or ñMr. Penaò), individually and on behalf of all others similarly situated, on personal knowledge of the facts respectively pertaining to himself and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against defendant British Airways, PLC (UK) (ñBAò or ñBritish Airwaysò).

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against BA for its failure to exercise reasonable care in securing and safeguarding its account holdersô Private Information (ñPrivate Informationò or ñPIò), specifically their names, billing addresses, email addresses, and credit card information, including credit card numbers, expiry dates and CVV codes.

2. BA is among the worldôs major airlines. It provides a platform available online and through mobile devices for customers to book and change their travel. Customers are led to believe and agree to provide Private Information, based on the fact that BA will safeguard

their Private Information, and that BA will share the information only with the persons, entities and groups with whom the customer consents.

3. However, on or about September 6, 2018, Plaintiff and Class members learned that commencing in or around August 2018, their Private Information was stolen from BAôs database storing Personal Information by hackers as a result of BAôs security failures.

4. BAôs security failures exposed Plaintiffôs and Class membersô Private Information to a massive security breach affecting hundreds of thousands of customers (the ñSecurity Breachò). The failures put Plaintiffôs and Class membersô personal and financial information and interests at serious, immediate, and ongoing risk.

5. The Security Breach was caused and enabled by BAôs knowing violation of its obligations to abide by best practices and industry standards concerning the security of its usersô Private Information. BA failed to comply with security standards and allowed its usersô Private Information to be compromised by cutting corners on security measures that should have been employed and could have prevented or mitigated the Security Breach that occurred.

II. JURISDICTION AND VENUE

6. The Court has jurisdiction over Plaintiffôs claims under 28 U.S.C. § 1332(d)(2) (ñCAFAò), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendantôs citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

7. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and 1391(c)(2) because the Plaintiff and many class members reside in this District, a large share of Defendantôs American operations occur within this District, and because BA is subject to

personal jurisdiction in New York. In addition, the events giving rise to plaintiffôs causes of action arose, in part, in this District.

III. PARTIES

Plaintiff

8. Plaintiff Ralph Pena is a resident of Flushing, Queens, in the State of New York. He regularly travels by air and holds Emerald status ï the highest tier ï with Oneworld Alliance, of which British Airways is a member. He purchased an airline ticket on British Airwaysô website on September 1, 2018 for a flight from Thailand to Japan. He purchased the ticket using a Citibank credit card. On September 17, 2018, Citibank sent Mr. Pena notification of a suspicious purchase for merchandise totaling $1,000, and the card was subsequently cancelled. The charge for merchandise was eventually refunded. When Citibank sent a replacement card, Mr. Pena was already away on a trip to Thailand with his wife. Had his credit card not been canceled after it was compromised, Mr. Pena would have used the credit card for transactions to accrue points, a feature that Mr. Pena greatly values and that he had to lose the valuable reward points. Mr. Pena would not have booked his ticket on British Airwaysô website had BA told him that it failed to maintain adequate computer systems and data security practices to safeguard his Private Information from theft.

9. Mr. Pena also changed dates on an existing ticket on British Airwaysô website on July 1, 2018. He paid using a Chase Ultimate Reserve Visa card. That card was compromised in August 2018 when Mr. Pena discovered that approximately 20 unauthorized Uber rides had been charged to the card. Mr. Pena had the card cancelled. Had his credit card not been canceled after it was compromised, Mr. Pena would have used the credit card for transactions

to accrue points, a feature that Mr. Pena greatly values and that he had to lose the valuable reward points.

10. Plaintiff is also at risk of imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

11. Plaintiff has a continuing interest in ensuring that his PI is protected and safeguarded from future breaches.

12. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PIð a form of intangible property that Plaintiff entrusted to Defendant that was compromised in and as a result of the Security Breach. Plaintiff was also forced to expend valuable time to rectify the loss of his card and privileges while overseas.

13. The injuries suffered by Plaintiff and Class members as a direct result of the Security Breach include:

a. theft of their personal and financial information;

b. improper disclosure of their PI;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PI being placed in the hands of criminals and potential sale of Plaintiffôs and Class membersô information on the Internet black market;

d. damages to and diminution in value of their PI entrusted to BA and the loss of Plaintiffôs and Class membersô privacy; and

e. loss of time from addressing the breach and loss of the value of cancelled credit cards, including loss of rewards points that would have accrued from the time of cardsô cancellation until a new card is issued.

Defendant

14. BAôs North American headquarters is in New York, New York.

15. JFK and Newark International Airport (ñEWRò) have the largest volume of BA passenger traffic in the United States. JFK is located within the Eastern District of New York, and EWR is located approximately 15 miles from 225 Cadman Plaza East, Brooklyn, NY 11201.

16. BAôs 2017 revenue exceeded $16 billion. Of that, over $2.5 billion in sales originated in the United States.

17. BA, a subsidiary of the International Consolidated Airlines Group S.A. (ñIAGò), is incorporated under the law of England and Wales. Its principal place of business and corporate headquarters is in Harmondsworth, West Drayton, United Kingdom.

IV. FACTUAL BACKGROUND

18. BA has long prided itself as at the vanguard of international connection, technological advancement and customer care. It is the successor of Imperial Airways, which flew across the British Empire, beginning in 1919. Its longstanding motto was ñ[t]he worldôs favourite airline.ò until 2011 when it was changed to ñ[t]o fly, to serve.ò In the wake of severe cost cutting measures in recent years, BAôs actual motto could be, as one commentator put it: ñTo fly, to shave (costs).ò The present era of austerity at BA has not just compromised customer satisfaction, but handed sensitive customer data to thieves as well.

19. Thousands of American consumers book travel on BAôs web platform every year. Operation of just a single BA flight route between New York and London yielded a whopping $1,037,724,867 between April 1, 2017 to March 31, 2018.[1] With customers sharing their Private Information to book travel, BA oversees an exceptionally large number of online financial transactions involving sensitive personal data.

20. BA has long known the critical importance of protecting usersô Private Information from unauthorized access. BA also knows the multitude of harms that foreseeably flow to individual users when information is stolen or misused by criminals. As it said in its 2017 annual report: ñThe Group could face financial loss, disruption or damage to brand reputation arising from an attack on our systems é . If we do not adequately protect our customer and employee data, we could breach regulation and face penalties and loss of customer trust.ò[2]

21. To its users, BA promotes and provides assurances that their data is safe and secure when making transactions with BA. BAôs privacy policy[3] makes the following representations (ñPrivacy Security Representationsò):

- ñBritish Airways is committed to respecting your privacy and protecting your personal informationò
- ñWe will put in place measures to protect your information and keep it secureò

[1] Forbes, ñNew York-London Is the Worldôs First Billion-Dollar Airline Route,ò Dan Reed (July 9, 2018), available at https://www.forbes.com/sites/danielreed/2018/07/09/for-real-new-york-london-is-the-worlds-first-billion-dollar-route-for-british-airways/#39d6ae2580b6 (last accessed October 16, 2018).

[2] British Airways Plc, ñAnnual Report and Accounts Year ended 31 December 2017,ò available at goo.gl/3LM9RW (last accessed October 16, 2018).

[3] British Airways, ñPrivacy Policy ï Our Privacy Promise,ò available at https://www.britishairways.com/en-us/information/legal/privacy-policy (last accessed Oct. 16, 2018).

- ñWe will respect your data protection rights and aim to give you control over your own information.ò
- ñWe take great care to protect the personal information you provide to us.ò

22. BAôs statement on website security[4] also contains many representations about the strength of its data security systems:

- ñBooking online with British Airways is quick and easy.[5] British Airways makes every effort to maintain customer confidentiality when securing an online payment. This includes ensuring the security of your credit card details and other personal information.ò
- ñHow we secure your payment information when you book online. When you buy a British Airways ticket over the Internet, your web browser connects with the website through an SSL (ñSecure Sockets Layerò). SSL is an industry-standard protocol for encryption over the Internet.ò
- ñAll of your personal information is encrypted as it travels over the Internet, to and from www.ba.com. When information is encrypted, it is scrambled between your computer and our server. The information is only unscrambled when it safely reaches us. It's fast and safe, and it ensures that your personal information cannot be read by anyone else.ò
- ñCompleting the transaction. When you send your personal details to us, none of the information is stored on the website, it is passed straight back to our

[4] British Airways, ñWebsite Security,ò available at https://www.britishairways.com/en-us/information/legal/website-security (last updated September 2018) (last accessed October 16, 2018).

[5] A previous version of the statement read: ñBooking online with British Airways is quick, easy, convenient and safe.ò *See* *https://web.archive.org/web/20171029081658/www.britishairways.com/en-us/information/legal/website-security* (last updated September 2016) (last accessed October 16, 2018).

secure servers at our Heathrow headquarters, where it only exists as part of the record of your transaction.ò

- ñIf you see a security message during the booking process, it is simply informing you that you are entering a secure area of the site. You will also see this message when you are severing the connection with our secure server, and moving into an open, public area of the site. At this point all of your personal information has been deleted, whether or not you actually completed a purchase. Your browser can be configured to display this message or not, as you choose.ò
- ñYour personal information. British Airways considers your privacy to be of the utmost importance, and we are governed by the UK Data Protection Act 1998. If you are concerned with how we might collect and use information about you, you can find a complete explanation in our Privacy Policy.ò

23. BAôs annual financial report makes additional Privacy Security Representations about the strength of its data security systems, including that ñBA follows the IAG initiatives to enhance defences and response plans. The Group ensures that it is up to date with industry standards and address identified weaknesses. There is oversight of critical systems and suppliers to ensure that data is secure, and the Group adheres to regulations and understands the data that is held. A General Data Protection Regulation (GDPR) programme is in place and actions underway to confirm compliance to the new regulations which are effective May 2018.ò[6]

[6] British Airways Plc, ñAnnual Report and Accounts Year ended 31 December 2017,ò available at goo.gl/3LM9RW (last accessed October 16, 2018).

24. Defendantôs Privacy Security Representations are and were untrue. On information and belief, Defendant failed, and continues to fail, to provide adequate protection of its usersô personal and confidential information and has egregiously failed to provide sufficient and timely notice or warning of potential and actual cybersecurity breaches to its customers.

The BA Data Breach: A Foreseeable and Preventable Crisis

25. On September 6, 2018, BA announced that sensitive personal and payment PI of its customers was compromised in a data breach. BA disclosed that information had been stolen from 382,000 transactions made on its website and through its mobile application between August 21, 2018 and September 5, 2018. BAôs Chief Executive Alex Cruz described the attack as involving ñvery sophisticated efforts.ò

26. In reality, however, hackers used just 22 lines of code to lift customer data entered into a payment form.[7] The breach could have been prevented had BA lived up to the promises it made about data security. Adherence to industry standards and GDPR, as well as ñtak[ing] great care to protectò customer information and ñmak[ing] every effort to maintain customer confidentiality when securing an online payment,ò would have prevented the breach. Instead, sound data security practices fell victim to the cost-cutting axe that BA management has taken to its operations.

27. For years, warnings blared that BA needed to take the integrity of its information systems seriously.

[7] Lily Hay Newman, ñHow Hackers Slipped by British Airwaysô Defenses,ò Wired, available at https://www.wired.com/story/british-airways-hack-details/ (Sept. 11, 2018) (last accessed October 16, 2018).

28. For example, in May 2017, a breakdown of BAôs information technology systems led to the cancellation of hundreds of flights.[8] One affected passenger captured the ensuing disarray:

> ñItôs chaos, people are running about all over the place trying to rebook,ò she said. ñThereôs no one to help, no leadership. There are lots of people everywhere. Thereôs nowhere to sit, so people are just lying on the floor, sleeping on yoga mats.ò[9]

29. In July 2018, another IT failure caused the cancellation of hundreds of flights, affecting 10,000 passengers.[10] The failure was attributable to an outage of a third-party travel technology supplier, Amadeus, who BA outsourced to and who otherwise primarily provides flight booking software to budget airlines.[11]

30. BA was also on notice that it needed to revamp its data protection efforts. In July 2018, news reports documented that BA was asking consumers who had complained on Twitter to post their sensitive Private Information in order to ñcomply with GDPR.ò GDPR is the General Data Protection Regulation, the EUôs sweeping consumer privacy law that is intended to protect consumers from the nonconsensual disclosure of their Private Information by companies.[12] Obviously, compliance with GDPR does not compel companies to have their consumers post sensitive Private Information online. To make matters worse, the security

[8] Haroon Siddique, ñBritish Airways: turmoil continues after IT failure grounds flights,ò The Guardian, available at https://www.theguardian.com/business/2017/may/28/british-airways-cyber-attack-unlikely-amid-scramble-to-resume-flights-on-sunday (May 28, 2017).

[9] *Id.*

[10] Simon Calder, ñBritish Airways Chaos at London Heathrow as Cancelled and Delayed Flights Affect 10,000 Passengers,ò The Independent, available at https://www.independent.co.uk/travel/news-and-advice/heathrow-airport-british-airways-flights-cancelled-passengers-it-problems-london-latest-a8454061.html (July 19, 2018) (last accessed Oct. 16, 2018).

[11] Gareth Corfield, ñBritish Airwaysô latest Total Inability to Support Upwardness of Planes* caused by Amadeus system outage,ò The Register (July 19, 2018), available at https://www.theregister.co.uk/2018/07/19/amadeus_british_airways_outage_load_sheet/ (last accessed October 17, 2018).

[12] Nick Statt, ñBritish Airways asked customers to post personal information on Twitter ćto comply with GDPR,ò The Verge (July 19, 2018), available at https://www.theverge.com/2018/7/19/17591732/british-airways-gdpr-compliance-twitter-personal-data-security (last accessed October 17, 2018).

researcher who first posted about BAôs strange requests only discovered the problem because he sought to complain about the fact that he was only permitted to check-in online after disabling adblocker. This was done by BA so that booking details could be revealed to third party advertisers. As he noted, this was done without consent, which is, ironically, a violation of GDPR.[13]

31. BA failed to heed the warnings and its customers paid the price when hackers were able to steal their sensitive Private Information in the recent data breach.

32. As stated above, the customer information taken included: names, billing addresses, email addresses, and credit card information, including credit card numbers, expiry dates and, perhaps most troubling, CVV codes. CVV codes are not to be saved at any time, which means that the hackers were able to take them from live transactions or, alternatively, BA was storing them in violation of well-established security standards.

33. Commenters have noted that the nature of the data breach, particularly the stealing of CVV codes, indicates that BA was not following industry standards and requirements.[14] Specifically, the Payment Card Industry Data Security Standard (PCI DSS) is a well-established information security standard for entities that deal with credit cards. PCI DSS sets forth the following requirements:

- ñDo not store the card verification code or value (three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.ò

[13] *Id.*

[14] *See* Fouad Khalil, ñBritish Airways breach shows the need for ócontinuous compliance,ôò (Sept. 17, 2018), available at https://www.paymentssource.com/opinion/british-airways-breach-will-test-old-school-data-compliance-practices (last accessed Oct. 17, 2018).

- ñUse strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.ò
- ñ[D]evelop and maintain secure systems and applications.ò
- ñ[Conduct] regular tests of security systems and processes.ò

34. Had BA followed these PCI DSS requirements, the hackers could not have breached BAôs systems to steal customer data, particularly the CVV codes.

35. To steal customer data, hackers ñlikely used a ócross-site scriptingô attack, in which bad actors identify a poorly secured web page component and inject their own code into it to alter a victim siteôs behavior.ò Here, the target script was connected to a BA baggage claim page that had not been updated since 2012. The hackers inserted a mere 22 lines of code to lift customer data typed into payment forms. They used similar code to compromise BAôs mobile application. WIRED aptly observed that ñ[w]hile the attack wasnôt elaborate, it was effective é .ò[15]

36. Just days ago, British Airways announced that an internal investigation has revealed that the data breach is far greater than originally believed.[16] This breach affected customers who booked travel between April 21 and July 28, 2018. British Airwaysô statement said that the name, billing address, email address, card payment information, including card number, expiry date and CVV were potentially compromised.

37. The European Union, the British government, and the federal and state governments of the United States have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The EUôs GDPR affirms a fundamental right and freedom of individuals to the

[15] https://www.wired.com/story/british-airways-hack-details/

[16] Derek Kortepeter, ñBritish Airways Data Breach Bigger than Originally Thought,ò available at http://techgenix.com/british-airways-data-breach/ (Nov. 1, 2018).

protection of personal data (Art. 1) and establishes that personal data shall be ñprocessed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing é .ò (Art. 5). It requires businesses to ñimplement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including é the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; é a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.ò (Art. 32). It adds that ñ[i]n assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from é unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.ò (Art. 32). The GDPR made clear the prime importance of data security practices, and it was common knowledge that businesses must take appropriate measures to become compliant. *See, e.g.,* Barney Thompson, ñWake-up call to business with one month to be GDPR-compliant,ò Financial Times (April 24, 2018), available at https://www.ft.com/content/ee98973a-47d4-11e8-8ee8-cae73aab7ccb (last accessed Nov. 1, 2018).

38. The United Kingdomôs Information Commissionerôs Office released a comprehensive guide to the GDPR as well as toolkits to assist businesses in protecting data security.[17] This further underscored the importance of implementing appropriate data security measures.

[17] *See https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr*

39. In the U.S., the FTC has issued numerous guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[18]

40. In 2016, the FTC updated its publication, *Protecting Private Information : A Guide for Business*, which establishes guidelines for fundamental data security principles and practices for business.[19] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of Private Information that is no longer needed; encrypt information stored on computer networks; understand their networkôs vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

41. The FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[20]

42. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as

[18] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited April 4, 2018).

[19] Federal Trade Commission, *Protecting Private Information : A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 4, 2018).

[20] Federal Trade Commission, *Start With Security*, *supra* n. 6.

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (ñFTCAò), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

43. BA was at all times fully aware of its obligation to protect the Private Information of its account holders. BA was also aware of the significant repercussions if it failed to do so because it collected Private Information to process transactions and knew that this data, if hacked, would result in injury to Plaintiff and Class members.

Security Breaches Lead to Identity Theft

44. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.[21]

45. Similarly, the FTC cautions that identity theft wreaks havoc on consumersô finances, credit history, and reputation and can take time, money, and patience to resolve.[22] Identity thieves use stolen Private Information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[23]

46. Private Information is a valuable commodity to identity thieves. Plaintiffôs and Class membersô Private Information can be sold and traded by cyber criminals on the dark web. Criminals often trade the information on the dark web for a number of years.

[21] *See Victims of Identity Theft, 2014*, DOJ, at 1 (2015), available at https://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited September 18, 2018).

[22] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, at 3 (2012), available at http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited September 18, 2018).

[23] The FTC defines identity theft as ña fraud committed or attempted using the identifying information of another person without authority.ò 16 C.F.R. § 603.2. The FTC describes ñidentifying informationò as ñany name or number that may be used, alone or in conjunction with any other information, to identify a specific person,ò including, among other things, ñ[n]ame, social security number, date of birth, official State or government issued driverôs license or identification number, alien registration number, government passport number, employer or taxpayer identification number.ò *Id*.

47. The National Institute of Standards and Technology categorizes the combination of names and credit card numbers as sensitive and warranting a higher impact level based on the potential harm when used in contexts other than their intended use.[24] Private information that is ñlinkedò or ñlinkableò is also more sensitive. Linked information is information about or related to an individual that is logically associated with other information about the individual. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. An example of linking information the NIST report cites is a Massachusetts Institute of Technology study showing that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth.

48. Private information is broader in scope than directly identifiable information. As technology advances, computer programs become increasingly able to scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible.

49. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[25] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

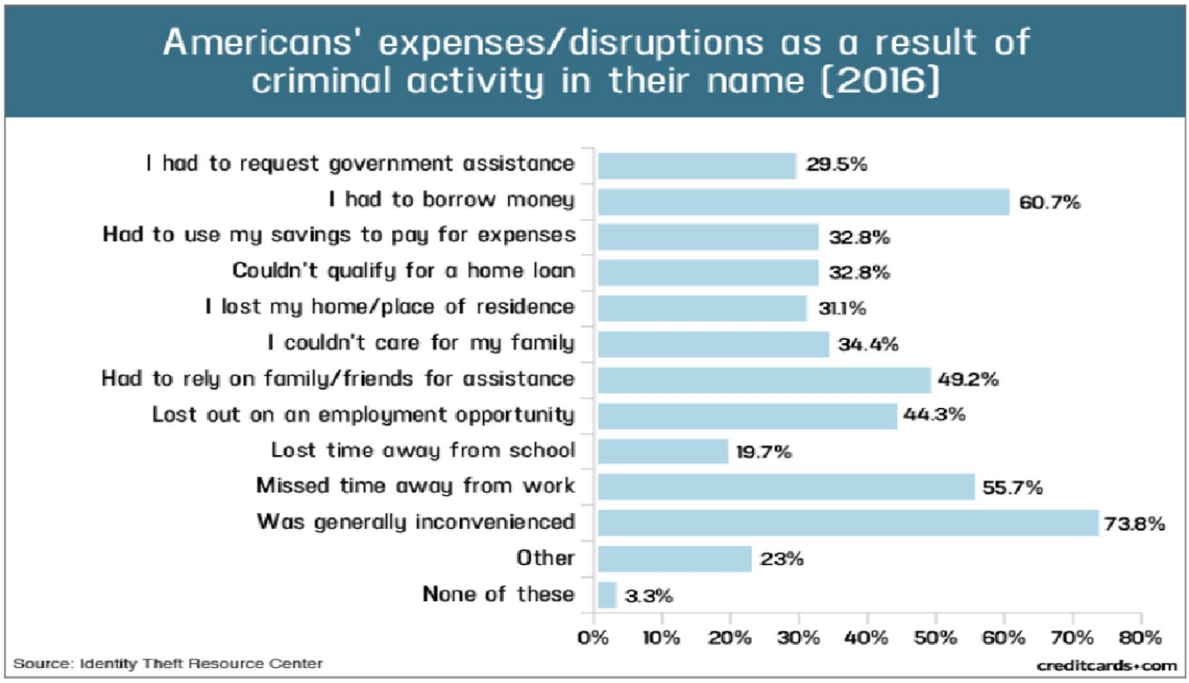
---

[24] Erika McCallister, et al., *Guide to Protecting the Confidentiality of Personally Identifiable Information (PI)*, National Institute of Standards and Technology Special Publication 800-122, 3-3, available at http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=904990 (last visited September 18, 2018).

[25] *Supra,* n.16.

50. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.ò[26]

51. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Private Information :[27]



V. CLASS ACTION ALLEGATIONS

52. Plaintiff brings all counts, as set forth below, on behalf of himself and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a Nationwide Class defined as:

[26] *See* Department of Justice, *Victims of Identity Theft, 2014*, *supra* n. 11 at 6 .

[27] Source: ñCredit Card and ID Theft Statisticsò by Jason Steele, available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited September 18, 2018).

> All persons in the United States who used British Airwaysô website or mobile application to make a payment, including for purchase of a ticket or for a change in travel, at any time between August 21 and September 5, 2018 (the ñNationwide Classò).

53. In the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the laws of the State of New York, and on behalf of the New York Subclass, defined as follows:

> All persons in New York who used British Airwaysô website or mobile application to make a payment, including for purchase of a ticket or for a change in travel, at any time between August 21 and September 5, 2018. (the ñNew York Subclassò).

54. Excluded from the Class and Subclass are Defendant and its affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

55. Certification of Plaintiffôs claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

56. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class and Subclass are so numerous that joinder of all Class members would be impracticable. On information and belief, Class and Subclass members number in the thousands.

57. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all Class and Subclass members and predominate over questions affecting only individual Class and Subclass members. Such common questions of law or fact include, *inter alia*:

a. Whether BA failed to use reasonable care and commercially reasonable methods to secure and safeguard Plaintiffôs and Class and Subclass membersô Private Information;

b. Whether BA properly implemented its purported security measures to protect Plaintiffôs and Class and Subclass membersô Private Information from unauthorized capture, dissemination, and misuse;

c. Whether BA took reasonable measures to determine the extent of the Security Breach after it first learned of same;

d. Whether BAôs conduct constitutes breach of an implied contract;

e. Whether BA willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffôs and Class and Subclass membersô Private Information;

f. Whether BA was negligent in failing to properly secure and protect Plaintiffôs and Class and Subclass membersô Private Information;

g. Whether Plaintiff and the other members of the Class and Subclass are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief;

h. Whether BA engaged in conduct in violation of New Yorkôs GBL 349 & 350 by its conduct;

i. Whether Plaintiff and class are entitled to statutory damages.

58. BA engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other Class and Subclass members. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

59. **Typicality—Federal Rule of Civil Procedure 23(a)(3).**

Plaintiffôs claims are typical of the claims of the other Class and Subclass members because, among other things, all Class members were similarly injured through BAôs uniform misconduct described above and were thus all subject to the Security Breach alleged herein. Further, there are no defenses available to BA that are unique to Plaintiff.

60. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate Class and Subclass representatives because his interests do not conflict with the interests of the other Class and Subclass members he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Classô and Subclassô interests will be fairly and adequately protected by Plaintiff and his counsel.

61. **Insufficiency of Separate Actions—Federal Rule of Civil Procedure 23(b)(1).** Absent a representative class action, members of the Class and Subclass would continue to suffer the harm described herein, for which they would have no remedy. Even if separate actions could be brought by individual consumers, the resulting multiplicity of lawsuits would cause undue hardship and expense for both the Court and the litigants, as well as create a risk of inconsistent rulings and adjudications that might be dispositive of the interests of similarly situated consumers, substantially impeding their ability to protect their interests, while establishing incompatible standards of conduct for BA. The Class and Subclass thus satisfy the requirements of Fed. R. Civ. P. 23(b)(1).

62. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class and Subclass, making injunctive and/or declaratory relief appropriate with respect to the classes under Fed. Civ. P. 23 (b)(2).

63. **Superiority—Federal Rule of Civil Procedure 23(b)(3).**

A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class and Subclass members are relatively small compared to the burden and expense that would be required to individually litigate their claims against BA, so it would be impracticable for Class members to individually seek redress for BAôs wrongful conduct. Even if Class and Subclass members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

VI. CAUSES OF ACTION

COUNT I

(Negligence)
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the New York Subclass)

64. Plaintiff repeats and re-alleges the allegations contained in the foregoing paragraphs as though fully set forth herein.

65. BA owes numerous duties to Plaintiff and the other members of the Class. These duties include:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect Private Information in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and the other members of the Class of the Security Breach.

66. BA knew or should have known the risks of collecting and storing Private Information and the importance of maintaining secure systems. BAôs own Privacy Security Representations demonstrate it is well aware of these risks and its duty to implement adequate security systems protocols and practices.

67. BA knew or should have known that its security practices did not adequately safeguard Plaintiffôs and the other Class membersô Private Information.

68. BA breached the duties it owes to Plaintiff and Class members in several ways, including:

a. failing to implement adequate security systems, protocols and practices sufficient to protect BA usersô Private Information and thereby creating a foreseeable risk of harm;

b. failing to comply with the minimum industry data security standards during the period of the Security Breach; and

c. failing to timely and accurately disclose to BA users that their Private Information had been improperly acquired or accessed.

69. But for BAôs wrongful and negligent breach of the duties it owed to Plaintiff and the other Class members, their Private Information would not have been compromised.

70. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of BAôs negligent conduct.

COUNT II

(Breach of Implied Contract)
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the New York Subclass)

71. Plaintiff repeat and re-alleges the allegations contained in the foregoing paragraphs as though fully set forth herein.

72. In making a financial transaction on BAôs website or mobile application, Plaintiff and the other members of the Class entered into an implied contract with BA, whereby BA became obligated to reasonably safeguard Plaintiffôs and the other Class membersô Private Information.

73. Under the implied contract, BA was obligated to not only safeguard the Private Information, but also to provide Plaintiff and the other Class members with prompt, truthful, and adequate notice of any security breach or unauthorized access of said information.

74. BA breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their Private Information.

75. BA also breached its implied contract with Plaintiff and the other Class members by failing to provide prompt, truthful, and adequate notice of the Security Breach and unauthorized access of their Private Information by hackers.

76. Plaintiff and the other Class members suffered and will continue to suffer damages including, but not limited to: (i) improper disclosure of their Private Information; (ii) the increased risk of identity theft; and (iii) deprivation of the value of their Private Information, which is likely to be sold to cyber criminals on the dark web.

COUNT III

Violations of N.Y. Gen. Bus. Law § 349
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the New York Subclass)

77. Plaintiff, individually and on behalf of Class and Subclass members, repeats and re-alleges the allegations contained in the foregoing paragraphs as though fully set forth herein.

78. New York General Business Law (ñNYGBLò) § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

79. By reason of the conduct alleged herein, Defendant engaged in unlawful and deceptive practices within the meaning of the NYGBL § 349. The conduct alleged herein is a ñbusiness practiceò within the meaning of the NYGBL § 349.

80. Defendant pledged to adhere to industry standards, take great care to protect customer information, and make every effort to maintain customer confidentiality when securing an online payment.

81. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied ñwith federal regulationsò and that would have kept Plaintiffôs and Class membersô Private Information secure, preventing loss or misuse. Defendant did not disclose to Plaintiff and the Class members that its data systems were not secure.

82. Plaintiff and Class Members never would have provided their sensitive and Private Information if they had been told or knew that BA failed to maintain sufficient security to keep such Private Information from being hacked and taken by others.

83. Defendant violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendantôs many systems and services, specifically

the security thereof, and its ability to allow Plaintiff and Class Members to safely disclose their Private Information to make transactions.

84. Defendant also violated NYGBL §349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiff and the Class Members of the Security Breach. If Defendant had complied with these legal requirements, Plaintiff and the Class Members would not have suffered the damages related to the Security Breach.

85. BAôs practices, acts, policies and course of conduct violate NYGBL § 349 in that:

a. BA actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and the Class at the time they provided such Private Information that BA did not have sufficient security or mechanisms to protect personal Private Information;

b. BA failed to give adequate warnings and notices regarding the defects and problems with its system(s) of security systems that it maintained to protect Plaintiffôs and the Classôs Private Information. BA possessed prior knowledge of the inherent defects in its IT systems and failed to address the same or to give adequate and timely warnings that there had been a Security Breach;

c. BA violated GBL Sec-889-aa, et. seq.

86. Plaintiff and the Class were entitled to assume, and did assume, Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose at any time that Plaintiffôs and the Classô Private Information was vulnerable to hackers because Defendantôs data security measures were inadequate, and Defendant was the only one in possession of that material information, which it had a duty to disclose.

87. The aforementioned conduct is and was deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that BA has, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the defective security system it maintained and failed to reveal the Security Breach timely and adequately.

88. Defendant should not have made the Privacy Security Representations that it did if it did not, in fact, adhere to such policies.

89. Members of the public were deceived by and relied upon BAsô affirmative misrepresentations and failures to disclose.

90. Such acts by BA are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to BA. Said deceptive acts and practices are material. The requests for and use of such Private Information was a consumer-oriented act and thereby falls under the New York consumer fraud statute, NYGBL § 349.

91. Furthermore, as alleged above, Defendantôs failure to secure Plaintiffôs and the ClassôPrivate Information violates the FTCA and therefore violates NYGBL § 349.

92. BAôs wrongful conduct caused Plaintiff and the Class to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the Private Information by third parties and placing the Plaintiff and the Class at serious risk for monetary damages.

93. As a direct and proximate result of BAôs violations of the above, Plaintiff and Class Members suffered damages including, but not limited to:

a. theft of their personal and financial information;

b. improper disclosure of their Private Information;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and potential sale of Plaintiffôs and Class membersô information on the Internet black market; and

d. damages to and diminution in value of their Private Information entrusted to BA and the loss of Plaintiffôs and Class membersôprivacy.

94. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the Class seek statutory damages for each injury and violation which has occurred.

COUNT IV

(Violation of New York's Data Breach Laws – Delayed Notification)
(N.Y. Gen. Bus. Law § 899-aa)
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the New York Subclass)

95. Plaintiff, individually and on behalf of the other New York Subclass members, repeat and re-allege the allegations contained in the foregoing paragraphs as though fully set forth herein.

96. Section 899-aa(3) of NYGBL requires any ñperson or business which maintains computerized data which includes private information which such person or business does not own shall notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, acquired by a person without valid authorization.ò

97. Section 899(5) of NYGBL states:

> The notice required by this section shall be directly provided to the affected persons by one of the following methods:
>
> (a) written notice;

> (b) electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the person or business who notifies affected persons in such form; provided further, however, that in no case shall any person or business require a person to consent to accepting said notice in said form as a condition of establishing any business relationship or engaging in any transaction;
>
> (c) telephone notification provided that a log of each such notification is kept by the person or business who notifies affected persons; or
>
> (d) Substitute notice, if a business demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such business does not have sufficient contact information. Substitute notice shall consist of all of the following:
>
> (1) e-mail notice when such business has an e-mail address for the subject persons;
>
> (2) conspicuous posting of the notice on such businessôs web site page, if such business maintains one; and
>
> (3) notification to major statewide media.

98. The Security Breach described in this Complaint constitutes a ñbreach of the security systemò of Defendant.

99. As alleged above, Defendant unreasonably delayed informing Plaintiff and the Class about the Security Breach, affecting the confidential and non-public Private Information of Plaintiff and the Class after Defendant knew the Security Breach had occurred.

100. Defendant failed to disclose to Plaintiff and the Class, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Private Information when Defendant knew or reasonably believed such information had been compromised.

101. Defendantôs ongoing business interests gave Defendant incentive to conceal the Security Breach from the public to ensure continued revenue.

102. Upon information and belief, no law enforcement agency instructed Defendant that notification to the Plaintiff and the Class would impede Defendantôs investigation.

103. As a result of Defendantôs violation of New York law, Plaintiff and the Class were deprived of prompt notice of the Security Breach and were thus prevented from taking appropriate protective measures. These measures would have prevented some or all of the damages Plaintiff and the Class suffered because their stolen information would not have any value to identity thieves.

104. As a result of Defendantôs violation of New York law, Plaintiff and the Class have suffered incrementally increased damages separate and distinct from those simply caused by the breaches themselves.

105. Plaintiff and the Class seek all remedies available under New York law, including, but not limited to damages the Plaintiff and the Class suffered as alleged above, as well as equitable relief.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of all claims so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against BA, as follows:

A. Declaring that this action is a proper class action, certifying the Class and Subclass as requested herein, designating Plaintiff as Class and Subclass Representative, and appointing Class Counsel as requested in Plaintiffôs motion for class certification;

B. Ordering BA to pay actual damages to Plaintiff and the other members of the Class and Subclass;

C. Ordering BA to pay punitive damages, as allowable by law, to Plaintiff and the other members of the Class and Subclass;

D. Ordering BA to pay attorneysô fees and litigation costs to Plaintiff and his counsel;

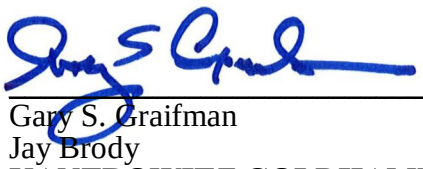
E. Ordering BA to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

F. Ordering BA to pay both pre- and post-judgment interest on any amounts awarded; and

G. Ordering such other and further relief as may be just and proper.

Date: November 5, 2018

Respectfully submitted,



Gary S. Graifman
Jay Brody
KANTROWITZ GOLDHAMER & GRAIFMAN, P.C.
747 Chestnut Ridge Rd.
Chestnut Ridge, NY 10977
Tel: (845) 356-2570
Fax: (845) 356-4335
ggraifman@kgglaw.com
jbrody@kgglaw.com

Nicholas A. Migliaccio
Jason S. Rathod (*pro hac vice* anticipated)

MIGLIACCIO & RATHOD LLP
412 H Street NE, Ste. 302
Washington, DC 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Attorneys for Plaintiff and the Putative Class and Subclass